NEW MEXICO DEPARTMENT OF HOMELAND SECURITY AND EMERGENCY MANAGEMENT (NMDHSEM)

Nonprofit Security Grant Program (NSGP) 2024
Funding Announcement and Allocation Methodology

1. Issued By

U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)/Grant Programs Directorate (GPD)

New Mexico Department of Homeland Security and Emergency Management (DHSEM)

2. Assistance Listings Number

97.008

3. Assistance Listings Title

Nonprofit Security Grant Program

4. Funding Opportunity Title

Fiscal Year 2024 Nonprofit Security Grant Program (NSGP)

5. Funding Opportunity Number

DHS-24-GPD-008-00-99

6. Authorizing Authority for Program

Section 2009 of the *Homeland Security Act of 2002* (Pub. L. No. 107-296, as amended) (6 U.S.C. 609a)

7. Appropriation Authority for Program

Department of Homeland Security Appropriations Act, 2024, Pub. L. No. 118-47, Title III, Protection, Preparedness, Response, and Recovery (2024 DHS Appropriations Act)

Table of Contents

A. Purpose

The Homeland Security Non-Profit Grant Program (NSGP) is a competitive grant program appropriated annually through the Department of Homeland Security (DHS) and administered by the Federal Emergency Management Agency (FEMA). It is intended to help nonprofit organizations increase their physical security posture against acts of terrorism as defined by law.

For FY 2024, DHS is focused on building a national culture of preparedness and protecting against terrorism and other threats to our national security. The threats to our Nation have evolved during the past two decades. We now face continuous cyber threats by sophisticated actors, threats to soft targets and crowded places, and threats from domestic violent extremists, who represent one of the most persistent threats to the nation today. Therefore, DHS/FEMA has identified one national priority area related to some of the most serious threats that recipients should address with their NSGP funds: **enhancing the protection of soft targets/crowded places**.

DHS is also focused on forging partnerships to strengthen information sharing and collaboration among federal, state, local, tribal, and territorial law enforcement. There are *no* requirements for information sharing between nonprofit organizations and law enforcement; however, the NSGP seeks to bring nonprofit organizations into broader state and local preparedness efforts by removing barriers to communication and being more inclusive. DHS/FEMA encourages information sharing, while the goal of the NSGP is centered on improving and increasing a nonprofit organization's physical/cyber security and facility/target hardening to enhance the protection of soft targets/crowded places. All NSGP activities must be linked to enhancing the security and safety at the physical site of the nonprofit organization.

B. Goal, Objectives, National Priorities

The NSGP will improve and increase the physical/cyber security and facility/target hardening of nonprofit organizations' facilities at risk of a terrorist of other extremist attack, ultimately safeguarding the lives and property of the American people. All NSGP activities must be linked to enhancing the security and safety at the physical site of the nonprofit organization. Concurrently, the NSGP will integrate the preparedness activities of nonprofit organizations that are at high risk of a terrorist or other extremist attack with broader state and local preparedness efforts.

The objective of the FY 2024 NSGP is to provide funding for physical and cybersecurity enhancements and other security-related activities to nonprofit organizations that are at high risk of a terrorist or other extremist attack within the period of performance. The NSGP also seeks to integrate the preparedness activities of nonprofit organizations with broader state and local preparedness efforts. Lastly, via funding spent on Planning, Organizational, Equipment, Training, and Exercises (POETE) towards enhancing the protection of soft targets and crowded places, the NSGP seeks to address and close capability gaps identified in individual nonprofit organization Vulnerability Assessments.

Given the evolving threat landscape, DHS/FEMA has evaluated the national risk profile and set priorities that help ensure appropriate allocation of scarce security dollars. In assessing the national risk profile for FY 2024, one area warrants the most concern under the NSGP:

- Enhancing the protection of soft targets/crowded places.

Likewise, there are several enduring security needs that crosscut the homeland security enterprise. The following

are second-tier priority areas that help recipients implement a comprehensive approach to securing communities:

- Effective planning;
- Training and awareness campaigns; and
- Exercises.

A continuing area of concern is the threat posed by malicious cyber actors. Additional resources and information regarding cybersecurity and cybersecurity performance goals are available through the Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals, and the National Institute of Standards and Technology.

NSGP Funding may be used for:

- Planning
- Organization
- Equipment
- Training
- Exercises
- Maintenance and Sustainment
- Contracted Security Personnel

FY 2024 NSGP Funding Priorities

All priorities in this table concern Safety and Security Lifelines.

NATIONAL PRIORITIES

Priority Areas	Core Capabilities Enhanced	Example Project Types
Enhancing the Protection of Soft Targets/Crowded Places	• Planning • Operational coordination • Public information and warning • Intelligence and Information Sharing • Interdiction and disruption • Screening, search, and detection • Access control and identity verification • Physical protective measures • Risk management for protection programs and activities • Cybersecurity • Long-term vulnerability reduction • Situational assessment • Infrastructure systems	• Private contracted security guards • Physical security enhancements ○ Closed circuit television (CCTV) security cameras ○ Security screening equipment for people and baggage ○ Access controls ▪ Fencing, gates, barriers, etc. ▪ Card readers, associated hardware/software • Cybersecurity enhancements ○ Risk-based cybersecurity planning and training ○ Improving cybersecurity of access control and identify verification systems ○ Improving cybersecurity of security technologies (e.g., CCTV systems) ○ Adoption of cybersecurity performance goals (https://www.cisa.gov/cpg)

ENDURING NEEDS

Priority Areas	Core Capabilities Enhanced	Example Project Types
Planning	• Planning • Risk management for protection programs and activities • Risk and disaster resilience assessment • Threats and hazards identification • Operational coordination	• Conduct or enhancement of security risk assessments • Development of: ○ Security plans and protocols ○ Emergency/contingency plans ○ Evacuation/shelter in place plans • Assessment of capabilities and gaps in planning for the needs of persons with disabilities and others with access and functional needs
Training & Awareness	• Long-term vulnerability reduction • Public information and warning	• Active shooter training, including integrating the needs of persons with disabilities • Security training for employees • Public awareness/preparedness campaigns
Exercises	• Long-term vulnerability reduction	• Response exercises

PERFORMANCE MEASURES

The performance metric for this program is:

- Percentage of funding awarded to the Soft Targets/Crowded Places national priority area by POETE (Planning, Organization, Equipment, Training, and Exercise) solution area, which includes:
  - Funding awarded for contract security;

- Funding awarded for target hardening;
- Funding awarded for cybersecurity measures; and
- Funding awarded for training, awareness campaigns, and exercises.

Funding spent on POETE towards enhancing the protection of soft targets and crowded places, the NSGP seeks to address and close capability gaps identified in individual nonprofit organization Vulnerability Assessments.

C. Subrecipient Eligibility

Nonprofit organizations eligible as **subapplicants to the State Administrative Agency (SAA)** are those organizations that are:

1. Described under section 501(c)(3) of the Internal Revenue Code of 1986 (IRC) and exempt from tax under section 501(a) of such code. ***This includes entities designated as "private" (e.g., private institutions of higher learning), as private colleges and universities can also be designated as 501c3 entities.***

Note: The Internal Revenue Service (IRS) does not require certain organizations such as churches, mosques, and synagogues to apply for and receive a recognition of exemption under section 501(c)(3) of the IRC. Such organizations are automatically exempt if they meet the requirements of section 501(c)(3).

These organizations are not required to provide recognition of exemption. For organizations that the IRS requires to apply for and receive a recognition of exemption under section 501(c)(3), the state may or may not require recognition of exemption, as long as the method chosen is applied consistently.
Refer to links below for additional information:

- Exemption Requirements - 501(c)(3) Organizations | Internal Revenue Service (irs.gov)
- Publication 557 (01/2022), Tax-Exempt Status for Your Organization | Internal Revenue Service (irs.gov)
- Charities and Nonprofits | Internal Revenue Service (irs.gov)

2. Able to demonstrate, through the application, that the organization is at high risk of a terrorist or other extremist attacks and
3. For NSGP-S, located outside of a FY 2024 UASI-designated highrisk urban area.

Examples of eligible subapplicant organizations can include houses of worship, museums, educational facilities, senior centers, community centers, and day camps, among many others.

ELIGIBILITY REQUIREMENTS:

Please note: ***Nonprofit organizations may*** **NOT** ***apply to FEMA directly***. The NMDHSEM, as the State Administrative Agency (SAA), is the only entity eligible to apply to DHS/FEMA for NSGP funds. Funds are then distributed to nonprofit organizations across the state utilizing a pass-through application process.

A. Eligible applicants must be registered in the federal System for Award Management (SAM) database and have a UEI (Unique Entity ID) number assigned to its agency (to get registered in the SAM database and request a UEI number, go to https://sam.gov/).
B. Eligible applicants must have an active/valid filing with the IRS to ensure 501(c)(3) status.
C. Failure to comply with program eligibility requirements may cause funds to be withheld and/or suspension or termination of grant funds.

D. Federal Award Information

FY 2024 New Mexico Target Allocation NSGP-S:	$1,852,500.00
5% for M&A based on Target Allocation:	$97,500.00
Maximum Amount of Award for each entity:	$150,000.00
Anticipated Funding Selection Date:	No later than September 30, 2024
Anticipated Award Date:	No Lather than October 31, 2024

E. Period of Performance

Projected Period of Performance Start Date:	January 1, 2025
Projected Period of Performance End Date:	June 30, 2027
Funding Instrument:	Sub-Grant Agreement from the SAA

F. Funding Methodology

The attached Fiscal Year 2024 Nonprofit Security Grant Program (NSGP) Subapplicant Quick Start Guide and the FY 2024 NSGP Notice of Funding Opportunity describes the steps taken by FEMA and NMDHSEM to allocate NSGP funding to stakeholders. These documents identify the priorities for funding so that subrecipients can be prepared to address the highest priority activities. They also serve as one way to increase transparency by sharing the decision-making approach with all stakeholders. Activities funded through NSGP have a Sub-grant Period of Performance that runs from January 1, 2025, to June 30, 2027.

MAXIMUM AWARD AMOUNT

Nonprofit organizations must apply through the New Mexico Department of Homeland Security and Emergency Management. Nonprofit organizations may only represent one site/location/physical address per application. For example, a nonprofit organization with one site may apply for up to $150,000 for that site.

Nonprofit organizations with multiple sites/locations/physical addresses may choose to apply for additional sites for up to $150,000 per site, for a maximum of three sites, *not to exceed $450,000 total* per nonprofit organization.

If a nonprofit subapplicant applies for projects at multiple sites, regardless of whether the projects are similar in nature, each individual site must include an assessment of the vulnerability and risk unique to each site. That is, one vulnerability assessment per location/physical address. Failure to do so may be cause for rejection of the application.

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

All costs charged to awards covered under the Fiscal Year 2024 Nonprofit Security Grant Program must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2C.F.R. Part 200, unless otherwise indicated in the NOFO, the terms and conditions of the award, or the FEMA Preparedness Grant Manual - 2024.

BUILD AMERICA, BUY AMERICA ACT (BABAA)

Build America, Buy America Act (BABAA), which was enacted as part of the Infrastructure Investment and Jobs Act §§ 70901-70927, Pub. L. No. 117-58 (2021); and Executive Order 14005, Ensuring the Future is Made in All of America by All of America's Workers. See also 2 C.F.R. Part 184 and Office of Management and Budget (OMB) Memorandum M-24-02, Implementation Guidance on Application of Buy America Preference in Federal Financial Assistance Programs for Infrastructure.

None of the funds provided under this program may be used for a project for infrastructure unless the iron and steel, manufactured products, and construction materials used in that infrastructure are produced in the United States.

The Buy America preference only applies to articles, materials, and supplies that are consumed in, incorporated into, or affixed to an infrastructure project. As such, it does not apply to tools, equipment, and supplies, such as temporary scaffolding, brought to the construction site and removed at or before the completion of the infrastructure project. Nor does a Buy America preference apply to equipment and furnishings, such as movable chairs, desks, and portable computer equipment, that are used at or within the finished infrastructure project but are not an integral part of the structure or permanently affixed to the infrastructure project.

For FEMA's official policy on BABAA, please see FEMA Policy 207-22-0001: Buy America Preference in FEMA Financial Assistance Programs for Infrastructure available at https://www.fema.gov/grants/policy-guidance/buy-america. To see whether a particular FEMA federal financial assistance program is considered an infrastructure program and thus required to include a Buy America preference, please see https://www.fema.gov/grants/policy-guidance/buy-america/programs-definitions.

G. Waivers

When necessary, subrecipients through DHSEM may apply for, and FEMA may grant, a waiver from these requirements.

A waiver of the domestic content procurement preference may be granted by the agency awarding official if FEMA determines that:

- Applying the domestic content procurement preference would be inconsistent with the public interest.
- The types of iron, steel, manufactured products, or construction materials are not produced in the United States in sufficient and reasonably available quantities or of a satisfactory quality.
- The inclusion of iron, steel, manufactured products, or construction materials produced in the United States will increase the cost of the overall project by more than 25%.

For FEMA awards, the process for requesting a waiver from the Buy America preference requirements can be found on FEMA's website at: https://www.fema.gov/grants/policy-guidance/buy-america.

H. Report issues of fraud, waste, abuse

Please note, when applying to this notice of funding opportunity and when administering the grant, applicants may report issues of fraud, waste, abuse, and mismanagement, or other criminal or noncriminal misconduct to

the Office of Inspector General (OIG) Hotline. The toll-free numbers to call are 1 (800) 323- 8603, and TTY 1 (844) 889-4357.

I. Protecting Houses of Worship and Public Venues

Across the United States, Americans congregate in faith-based venues to worship, learn, play, and bond as a community. However, public gatherings are vulnerable, and adversaries may perceive houses of worship as attractive targets where they can inflict mass casualties, cause substantial psychological impacts, and draw extensive media coverage. The DHS Center for Faith-Based & Neighborhood Partnerships (DHS Center) partners with interagency and whole community partners to offer numerous resources to assist faith-based and community organizations with their efforts to prepare for all types of hazards, whether natural or man-made. Technical assistance is provided through presentations, workshops, training, webinars, tabletop exercises, and training. Access to these free resources can be found at https://www.fema.gov/about/offices/faith.

J. Application Review Information

Nonprofit organizations must submit their FY 2024 NSGP-S applications to the New Mexico Department of Homeland Security and Emergency Management. FY 2024 NSGP-S applications will be reviewed through a two-phase state and federal review process for completeness, adherence to programmatic guidelines, feasibility, and how well the IJ (project description and justification) addresses the identified risk(s). For FY 2024 NSGP-S, SAAs will make recommendations to DHS/FEMA based on their target allocation and according to the chart listed in the NSGP-S Process subsection below.

The following are the FY 2024 NSGP-S evaluation process and criteria:

- For NSPG-S, verification that the nonprofit is located outside of one of the FY 2024 UASI-designated high-risk urban areas.
- Identification and substantiation of current or persistent threats or attacks (from within or outside the United States) by a terrorist or other extremist organization, network, or cell against the subapplicant based on their ideology, beliefs, and/or mission as: 1) an ideology-based/spiritual/religious; 2) educational; 3) medical; or 4) other nonprofit entity;
- Symbolic value of the site(s) as a highly recognized regional and/or national or historical institution(s) that renders the site a possible target of terrorist or other extremist attack;
- Role of the nonprofit organization in responding to or recovering from terrorist or other extremist attacks;
- Alignment between the project activities requested within the physical or cyber vulnerabilities identified in the organization's vulnerability assessment;
- Integration of nonprofit preparedness with broader state and local preparedness efforts;
- Completed IJ for each site that addresses an identified risk unique to that site, including the assessed threat, vulnerability, and consequence of the risk;
- Demonstration that the nonprofit organization is located within a disadvantaged community
- History of prior funding under NSGP. Not having received prior year NSGP funding is a positive factor when calculating the state score of the application.

Grant projects must be: 1) both feasible and effective at mitigating the identified vulnerability and thus reducing the risks for which the project was designed; and 2) able to be fully completed within the three-year period of performance. DHS/FEMA will use the information provided in the application, as well as any supporting documentation, to determine the feasibility and effectiveness of the grant project. Information that would assist in the feasibility and effectiveness determination includes the following:

- Scope of work (purpose and objectives of the project, identification of what is being protected);

- Desired outcomes, including expected long-term impact where applicable;
- Summary of status of planning and design accomplished to date (e.g., included in a capital improvement plan); and
- Project schedule.

Subrecipients are expected to conform, as applicable, with accepted engineering practices, established codes, standards, modeling techniques, and best practices.

FINANCIAL INTEGRITY CRITERIA

Prior to making a state and federal award, FEMA is required by 31 U.S.C. § 3354, as enacted by the Payment Integrity Information Act of 2019, Pub. L. No. 116-117 (2020); 41 U.S.C. § 2313; and 2 C.F.R. § 200.206 to review information available through any Office of Management and Budget (OMB)-designated repositories of governmentwide eligibility qualification or financial integrity information, including whether SAM.gov identifies the applicant as being excluded from receiving federal awards or is flagged for any integrity record submission. FEMA may also pose additional questions to the applicant to aid in conducting the pre-award risk review. Therefore, application evaluation criteria may include the following risk- based considerations of the applicant:

i. Financial stability.
ii. Quality of management systems and ability to meet management standards.
iii. History of performance in managing federal award.
iv. Reports and findings from audits.
v. Ability to effectively implement statutory, regulatory, or other requirements.

SUPPLEMENTAL FINANCIAL INTEGRITY CRITERIA AND REVIEW

Prior to making a federal award where the anticipated total federal share will be greater than the simplified acquisition threshold, currently $250,000:

a) FEMA is required by 41 U.S.C. § 2313 and 2 C.F.R. § 200.206(a)(2) to review and consider any information about the applicant, including information on the applicant's immediate and highest-level owner, subsidiaries, and predecessors, if applicable, that is in the designated integrity and performance system accessible through the System for Award Management (SAM), which is currently the Federal Awardee Performance and Integrity Information System (FAPIIS).
b) An applicant, at its option, may review information in FAPIIS and comment on any information about itself that a federal awarding agency previously entered.
c) FEMA will consider any comments by the applicant, in addition to the other information in FAPIIS, in making a judgment about the applicant's integrity, business ethics, and record of performance under federal awards when completing the review of risk posed by applicants as described in 2 C.F.R. § 200.206.

SECURITY REVIEW

DHS Intelligence and Analysis receives a list of potential NSGP subrecipient organizations, which it reviews against U.S. intelligence community reporting. The security review occurs after the competitive scoring and selection process is complete. The information provided for the security review is limited to the nonprofit organization's name and physical address, as submitted by the nonprofit organization. Any potentially derogatory information, as well as any potentially mitigating information, that could assist in determining whether a security risk exists is sent to FEMA and is used in making final award decisions.

K. NSGP -S Review and Selection Process

STATE REVIEW

Application packages are submitted by the nonprofit organization to the SAA based on the established criteria. The SAA will review applications and recommend to DHS/FEMA which nonprofit organizations should be selected for funding. As part of the state review, the SAAs must:

- Conduct an eligibility review;
- Verify that the nonprofit is located outside a FY 2024 UASI-designated high-risk urban area;
- Review and score all complete application packages (including vulnerability assessments and mission statement) using the NSGP Scoring Criteria provided by DHS/FEMA;
- Validate the self-certified organization type listed in the IJ by assessing the central purpose of the organization described in the mission statement;
- Prioritize all NSGP IJs by ranking each IJ. Each IJ will receive a unique rank (# 1 [one] being the highest ranked through the total number of applications the SAA scored);
- Submit the results of the state review along with complete investment justifications from eligible subapplicants to DHS/FEMA using the SAA Prioritization Tracker;
- Submit nonprofit organization application details for applications received but not recommended for funding (including incomplete applications and ineligible subapplicants), as well as justification as to why they are not being recommended for funding to DHS/FEMA using the SAA Prioritization Tracker (IJs for applications not being recommended for funding should not be submitted to FEMA);
- Submit IJs that are recommended for funding; SAAs should submit IJs that collectively represent 150% of the state's NSGP-S allocation; this will allow DHS/FEMA to award the next prioritized IJ in instances when a subapplicant is found to be ineligible or when a significant portion of an IJ includes proposed projects that are unallowable, for example:

NSGP-S Target Allocation	Submit IJs That Total This Amount to DHS/FEMA
$1.4 million	$2.1 million
$2 million	$3 million
$2.5 million	$3.75 million

- Submit IJs received and not recommended for funding, including incomplete IJs and IJs from subapplicants deemed ineligible.
- Retain the mission statements and vulnerability assessments submitted by each nonprofit organization.

The SAA will base the ranking on the final scores from the Prioritization Tracker as determined by the SAA's subject-matter expertise and discretion with consideration of the following factors:

- **Need:** The relative need for the nonprofit organization compared to the other subapplicants; and
- **Impact:** The feasibility of the proposed project and how effectively the proposed project addresses the identified need.

FEDERAL REVIEW

The IJs submitted by each SAA will be reviewed by DHS/FEMA federal staff. Federal staff will also verify that the nonprofit organization is located outside of a FY 2024 UASI-designated high-risk urban area. Federal reviewers will review each IJ to check for the following:

- Eligibility (e.g., that a potential subrecipient meets all the criteria for the program);
- Allowability of the proposed project(s); and

- Any derogatory information on the organization applying per "Security Review."

FINAL SCORE

To calculate an application's final score, the subapplicant's SAA score will be multiplied:

- By a factor of three for nonprofit groups that are at a high risk of terrorist or other extremist attacks due to their ideology, beliefs, or mission;
- By a factor of two for medical and educational institutions; and by a factor of one for all other nonprofit organizations.

Subapplicants who have never received a NSGP award will have 15 points added to their score. To advance considerations of equity in awarding NSGP grant funding, FEMA will add 10 additional points to the scores of organizations that are located within a disadvantaged community and demonstrate how they serve a disadvantaged community or population. FEMA will apply the Council on Environmental Quality's Climate and Economic Justice Screening Tool (CEJST), CEJST Geoplatform, to each subapplicant using the address of their physical location. FEMA will add 10 points to applications from organizations in communities identified as "disadvantaged" by CEJST.

Subapplicants will be selected from highest to lowest scored within their respective state/territory until the available state target allocation has been exhausted. In the event of a tie during the funding determination process, priority will be given to nonprofit organizations located in disadvantaged communities, then those that have not received prior year funding, and then those prioritized highest by their SAA. Should additional NSGP-S funding remain unobligated after reviewing all state/territory submissions, FEMA will use the final scores, in part, to determine how the remaining balance of funds will be allocated. Submissions will be selected for funding until the remaining balance of funds is exhausted.

DHS/FEMA will use the final results to make funding recommendations to the Secretary of Homeland Security. All final funding determinations will be made by the Secretary of Homeland Security, who retains the discretion to consider other factors and information in addition to DHS/FEMA's funding recommendations.

REQUIRED NOTICE OF NON-SELECTION

NMDHSEM is required to inform subapplicants of their non-selection no later than 90 days from the date NMDHSEM accepts their NSGP award.

DHSEM STANDARD TERMS AND CONDITIONS

All successful subapplicants for DHSEM grants are required to comply with DHSEM Standard Terms and Conditions. The applicable DHSEM Standard Terms and Conditions will be those in effect at the time the subaward was made. The terms and conditions that will apply for the subaward will be clearly stated in the subgrant agreement.

L. Administrative and National Policy Requirements

In addition to the requirements of in this section and in this NOFO, FEMA may place specific terms and conditions on individual awards in accordance with 2 C.F.R. Part 200.

In addition to the information regarding DHS Standard Terms and Conditions and Ensuring the Protection of Civil Rights, see the FEMA Preparedness Grant Manual - 2024 for additional information on administrative and national policy requirements, including the following:

- Environmental Planning and Historic Preservation (EHP) Compliance
- FirstNet
- National Incident Management System (NIMS) Implementation
- SAFECOM

ENSURING THE PROTECTION OF CIVIL RIGHTS

As the Nation works towards achieving the National Preparedness Goal, it is important to continue to protect the civil rights of individuals. Recipients and subrecipients must carry out their programs and activities, including those related to the building, sustainment, and delivery of core capabilities, in a manner that respects and ensures the protection of civil rights for protected populations.

Federal civil rights statutes, such as Section 504 of the Rehabilitation Act of 1973 and Title VI of the Civil Rights Act of 1964, along with DHS and FEMA regulations, prohibit discrimination on the basis of race, color, national origin, sex, religion, age, disability, limited English proficiency, or economic status in connection with programs and activities receiving federal financial assistance from FEMA, as applicable.

The DHS Standard Terms and Conditions include a fuller list of the civil rights provisions that apply to recipients. These terms and conditions can be found in the DHS Standard Terms and Conditions. Additional information on civil rights provisions is available at FEMA-CivilRightsOffice@fema.dhs.gov.

Monitoring and oversight requirements in connection with recipient compliance with federal civil rights laws are also authorized pursuant to 44 C.F.R. Part 7 or other applicable regulations.

In accordance with civil rights laws and regulations, recipients and subrecipients must ensure the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment.

ENVIRONMENTAL PLANNING AND HISTORIC PRESERVATION (EHP) COMPLIANCE

See the FEMA Preparedness Grant Manual - 2024 for information on EHP compliance.

NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS) IMPLEMENTATION

Subrecipients are highly encouraged to adopt and implement NIMS. Subrecipients are encouraged to reach out to their local Emergency Manager for assistance with establishing a NIMS implementation plan.

See the Preparedness Grants Manual for information about NIMS implementation.

MANDATORY DISCLOSURES

The non-Federal entity or applicant for a Federal award must disclose, in a timely manner, in writing to the Federal awarding agency or pass-through entity all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. (2 C.F.R. § 200.113)

Please note applicants and subrecipients may report issues of fraud, waste, abuse, and mismanagement, or other criminal or noncriminal misconduct to the Office of Inspector General (OIG) Hotline. The toll-free numbers to call are 1 (800) 323- 8603, and TTY 1 (844) 889-4357.

REPORTING

Subrecipients are required to submit various financial and programmatic reports as a condition of subaward acceptance. Future awards and funds drawdown may be withheld if these reports are delinquent.

MONITORING AND OVERSIGHT

The regulation at 2 C.F.R. § 200.337 provides DHS and any of its authorized representatives with the right of access to any documents, papers, or other records of the recipient [and any subrecipients] that are pertinent to a federal award in order to make audits, examinations, excerpts, and transcripts. The right also includes timely and reasonable access to the recipient's or subrecipient's personnel for the purpose of interview and discussion related to such documents. Pursuant to this right and per 2 C.F.R. § 200.329, DHS may conduct desk reviews and make site visits to review project accomplishments and management control systems to evaluate project accomplishments and to provide any required technical assistance. During site visits, DHS may review a recipient's or subrecipient's files pertinent to the federal award and interview and/or discuss these files with the recipient's or subrecipient's personnel. Recipients and subrecipients must respond in a timely and accurate manner to DHS requests for information relating to a federal award.

EQUAL RIGHTS

The FEMA Office of Equal Rights (OER) is responsible for compliance with and enforcement of federal civil rights obligations in connection with programs and services conducted by FEMA and recipients of FEMA financial assistance. All inquiries and communications about federal civil rights compliance for FEMA grants under this NOFO should be sent to FEMA-CivilRightsOffice@fema.dhs.gov.

ADDITIONAL INFORMATION

The Grants Program Directorate (GPD) has developed the Preparedness Grants Manual to guide applicants and recipients of grant funding on how to manage their grants and other resources. Recipients seeking guidance on policies and procedures for managing preparedness grants should reference the FEMA Preparedness Grant Manual - 2024 for further information. Examples of information contained in the FEMA Preparedness Grant Manual - 2024 include:

- Actions to Address Noncompliance
- Audits
- Case Studies and Use of Grant-Funded Resources During Real-World Incident Operations
- Community Lifelines
- Conflicts of Interest in the Administration of Federal Awards and Subawards
- Disability Integration
- National Incident Management System
- Payment Information
- Period of Performance Extensions
- Procurement Integrity
- Record Retention
- Whole Community Preparedness
- Report issues of Fraud, Waste, and Abuse
- Hazard Resistant Building Codes
- Other Post-Award Requirements

TERMINATION PROVISIONS

Pass-through entities should refer to 2 C.F.R. § 200.340 for additional information on termination regarding subawards. Note that all information in this Section H.1 "Termination Provisions" is repeated in the Preparedness Grants Manual.

NONCOMPLIANCE

If a subrecipient fails to comply with the terms and conditions of a state/federal award, DHSEM/FEMA may terminate the award in whole or in part. If the noncompliance can be corrected, DHSEM/FEMA may first attempt to direct the recipient to correct the noncompliance. This may take the form of a Compliance Notification. If the noncompliance cannot be corrected or the recipient is non-responsive, DHSEM/FEMA may proceed with a Remedy Notification, which could impose a remedy for noncompliance per 2 C.F.R. § 200.339, including termination. Any action to terminate based on noncompliance will follow the requirements of 2 C.F.R. §§ 200.341-200.342 as well as the requirement of 2 C.F.R. § 200.340(c) to report in FAPIIS the recipient's material failure to comply with the award terms and conditions. See also the section on Actions to Address Noncompliance in the FEMA Preparedness Grant Manual - 2024.

M. Application Evaluation Criteria and Process

An application submitted by an otherwise eligible nonprofit may be deemed ineligible when the person that submitted the application is not: 1) a *current employee, personnel, official, staff, or leadership* of the nonprofit organization; and 2) *duly authorized to apply* for an award on behalf of the nonprofit organization at the time of application.

Further, the Authorized Organization Representative (AOR) must be a duly authorized current employee, personnel, official, staff or leadership of the recipient and ***provide an email address unique to the subrecipient at the time of application and upon any change in assignment during the period of performance. Consultants or contractors of the recipient are not permitted to be the AOR of the recipient.***

Grant projects must be: 1) both feasible and effective at mitigating the identified vulnerability and thus reducing the risks for which the project was designed; and 2) able to be fully completed within the period of performance. The information provided in the application, as well as any supporting documentation, will be used to determine the feasibility and effectiveness of the grant project. Information that would assist in the feasibility and effectiveness determination includes the following:

- Scope of work (purpose, desired outcomes, and objectives of the project, identification of what is being protected);
- Including expected long-term impact where applicable;
- Summary of status of planning and design accomplished to date (e.g., included in a capital improvement plan); and
- Project schedule.

Recipients and subrecipients are expected to conform, as applicable, with accepted engineering practices, established codes, standards, modeling techniques, and best practices.

NSGP Investment Justification

Nonprofit subapplicants with one site may apply for up to $150,000 for that site. Non-Profit sub applicants with

multiple sites may apply for up to $150,000 per sit, for up to three sites with a maximum of $450,000 per nonprofit organization. If a nonprofit organization applies for multiple sites, it submit one complete investment justification per each site. IJ's cannot include more than one physical site.

The IJ must describe each investment proposed for funding. The investments or projects described in the IJ must:

1. Be for the location(s)/physical address(es) (NOT P.O. Boxes) that the nonprofit occupies at the time of application;
2. Address an identified risk, including threat and vulnerability, regardless of whether it is submitting for similar projects at multiple sites;
3. Demonstrate the ability to provide enhancements consistent with the purpose of the program and guidance provided by DHS/FEMA;
4. Be both feasible and effective at reducing the risks for which the project was designed;
5. Be able to be fully completed within the three-year period of performance; and
6. Be consistent with all applicable requirements outlined in this NOFO and the Preparedness Grants Manual.

Non profit subapplicants are required to self-identify with one for the following categories in the IJ as part of the application process:

a) Ideology-based/Spiritual/Religious
b) Educational
c) Medical
d) Other

VULNERABILITY/RISK ASSESSMENT

Each nonprofit subapplicant must include a vulnerability/risk assessment unique to the site the IJ is being submitted for.

MISSION STATEMENT

Each nonprofit subapplicant must include its Mission Statement and any mission implementation policies or practices that may elevate the organization's risk. SAAs will use the Mission Statement along with the nonprofit subapplicant's self- identification in the IJ to validate that the organization is one of the following types: 1) Ideology-based/Spiritual/Religious; 2) Educational; 3) Medical; or 4) Other. The organization type is a factor when calculating the final score of the application; see Section E "Application Review Information," subsection "Final Score."

FUNDING RESTRICTIONS AND ALLOWABLE COSTS

All costs charged to awards covered by this NOFO must comply with the Uniform Administrative Requirements, Cost Principles, and Audit Requirements at 2 C.F.R. Part 200, unless otherwise indicated in the NOFO, the terms and conditions of the award, or the Preparedness Grants Manual. This includes, among other requirements, that costs must be incurred, and products and services must be delivered, within the period of performance of the award. See 2 C.F.R. § 200.403(h) (referring to budget periods, which for FEMA awards under this program is the same as the period of performance).

Federal funds made available through this award may be used for the purpose set forth in this NOFO, the Preparedness Grants Manual, and the terms and conditions of the award and must be consistent with the statutory authority for the award. Award funds may not be used for matching funds for any other federal awards,

lobbying, or intervention in federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the Federal Government or any other government entity. See the Preparedness Grants Manual for more information on funding restrictions and allowable costs.

PROHIBITIONS ON EXPENDING FEMA AWARD FUNDS FOR COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES

See the FEMA Preparedness Grant Manual - 2024 for information on prohibitions on expending FEMA award funds for covered telecommunications equipment or services.

MANAGEMENT AND ADMINISTRATION (M&A) COSTS

M&A costs are allowed by the 2024 DHS Appropriations Act. M&A costs are for activities directly related to the management and administration of the award. M&A activities are those defined as directly relating to the management and administration of NSGP funds, such as financial management and monitoring. M&A expenses must be based on actual expenses or known contractual costs. Requests that are simple percentages of the award, without supporting justification, will not be allowed or considered for reimbursement. M&A costs for the NSGP are calculated as up to 5% of the total Federal award allocated to the subrecipient, not on final expenditures at close out.

M&A costs are not operational costs but are necessary costs incurred in direct support of the federal award or as a consequence of it, such as travel, meeting- related expenses, and salaries of full/part-time staff in direct support of the program. As such, M&A costs can be itemized in financial reports. Other M&A costs examples include preparing and submitting required programmatic and financial reports, establishing and/or maintaining equipment inventory, documenting operational and equipment expenditures for financial accounting purposes, and responding to official informational requests from state and federal oversight authorities.

NONPROFIT ORGANIZATION (SUBRECIPIENT) FOR NSGP-S

Nonprofit organizations that receive a subaward under the NSGP may use and expend up to 5% of each subaward for M&A purposes associated with that subaward. If an organization is receiving more than one subaward, they must be able to separately account for M&A costs for each subaward.

PLANNING

Planning costs are allowed under this program only as described in this funding notice and the FEMA Preparedness Grant Manual - 2024.

Funding may be used for security or emergency planning expenses and the materials required to conduct planning activities. Planning must be related to the protection of the facility and the people within the facility and should include consideration of access and functional needs as well as those with limited English proficiency. Planning efforts can also include conducting risk and resilience assessments on increasingly connected cyber and physical systems, on which security depends, the Resilience Planning Program | CISA and related CISA resources. Examples of planning activities allowable under this program include:

1. Development and enhancement of security plans and protocols;
2. Development or further strengthening of security assessments;
3. Emergency contingency plans;
4. Evacuation/Shelter-in-place plans;
5. Coordination and information sharing with fusion centers; and

6. Other project planning activities with prior approval from FEMA.

ORGANIZATION

Organization costs are not allowed under this program.

EQUIPMENT

Equipment costs are allowed under this program only as described in this funding notice and the FEMA Preparedness Grant Manual - 2024.

Allowable costs are focused on facility hardening and physical security enhancements. Funding can be used for the acquisition and installation of security equipment on real property (including buildings and improvements) owned or leased by the nonprofit organization, specifically in prevention of and/or protection against the risk of a terrorist or other extremist attack. This equipment is **limited to select items** on the Authorized Equipment List (AEL). These items, including the item's plain-language description *specific to the NSGP*, are as follows:

AEL Number	Title	Description
03OE- 03- MEGA	System, Public Address, Handheld or Mobile	Systems for mass audio notification, including vehicle-mounted high powered speaker systems, or battery powered megaphone/public address systems with corded microphone.
03OE-03- SIGN	Signs	Restricted access and caution warning signs that preprinted or field printable and can be various colors, sizes, and shapes. Examples can include traffic cones, other free-standing signage, mountable items, and signs and devices for individuals with disabilities and others with access and functional needs (e.g., programmable audible caution cones and scrolling marquis signs).
04AP-05- CRED	System, Credentialing	Software application and associated hardware and material for creating site/event credential badges and controlling scene access. Although some hardware may be required, functionality may also be obtainable via subscription as a cloud-based service, as opposed to purchasing software.
04AP-09- ALRT	Systems, Public Notification and Warning	Systems used to alert the public of protective actions or to provide warning to the public in the event of an incident, such as sirens, the Emergency Alert System (EAS), the Integrated Public Alert and Warning System (IPAWS), and Wireless Emergency Alerts (WEA).
04AP-11- SAAS	Applications, Software as a Service	Sometimes referred to as "on-demand software," this application runs on the provider's servers, delivering functionality via the internet to any device having connectivity and the required browser or interface. Access to the application is obtained via a service subscription rather than outright purchase, with all updates and configuration requirements handled by the service provider. *This item is limited to those services that support security systems such as access controls, camera networks, cybersecurity services or other critical infrastructure security.*
05AU-00- TOKN	System, Remote Authentication	Systems used to provide enhanced remote authentication, often consisting of a server or synchronization scheme and a device, token, or smartphone application.
05EN-00- ECRP	Software, Encryption	Encryption software used to protect stored data files or email

		messages.
05HS-00- MALW	Software, Malware/Anti-Virus Protection	Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments.
05HS-00- MALW	Software, Malware/Anti-Virus Protection	Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments.
05HS-00- PFWL	System, Personal Firewall	Personal firewall for operation on individual workstations. This item is usually a software solution, but appliances are also available. See also: 05NP-00-FWAL.
05NP-00- FWAL	Firewall, Network	Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL.
05NP-00- IDPS	System, Intrusion Detection/Prevention	Intrusion Detection and/or Prevention System deployed at either host or network level to detect and/or prevent unauthorized or aberrant (i.e, abnormal) behavior on the network.
06CP-01- PORT	Radio, Portable	Individual/portable radio transceivers, for notifications and alerts.
06CP-01- REPT	Repeater	Electronic device that receives a weak or low-level signal and retransmits that signal to extend usable range.
06CC-02- PAGE	Services/Systems, Paging	Paging services/systems/applications; one-way text messaging for notifications or alerts.
06CP-03- ICOM	Intercom/Intercom System	Communication system for a limited number of personnel in close proximity to receive alerts or notifications
06CP-03- PRAC	Accessories, Portable Radio	Speaker/microphone extensions to portable radios.
10GE-00- GENR	Generators	Generators (gasoline, diesel, propane, natural gas, etc.) and their required installation materials, including 10PE-00-PTSW (a power switch) if not already included, to support a redundant power supply for security systems, alarms, lighting, and other physical security/cybersecurity infrastructure or systems.
13IT-00- ALRT	System, Alert/Notification	Alert/notification software that allows for real-time dissemination of information for situational awareness or alerts among a group via means such as smartphones, landlines, pagers, etc. This item may also be a subscription cloud-based service using a web browser interface or a mobile application instead of a software.
10PE-00- UPS	Supply, Uninterruptible Power (UPS)	Systems that compensate for power loss to serviced equipment (e.g., short-duration battery devices, standby generator devices for longer duration).
14CI-00- COOP	System, Information Technology Contingency Operations	Back-up computer hardware, operating systems, data storage, and application software necessary to provide a working environment for contingency operations. May be a purchased as a remote service or a dedicated alternate operating site.
14EX-00- BCAN	Receptacles, Trash, Blast-Resistant	Blast-resistant trash receptacles.
14EX-00- BSIR	Systems, Building, Blast/Shock/Impact Resistant	Systems to mitigate damage from blasts, shocks, or impacts, such as column and surface wraps, wall coverings, portable or fix ballistic boards/barriers, breakage/shatter resistant glass, window wraps/films/velums, etc.
14SW-01- ALRM	Systems/Sensors, Alarm	Systems and standalone sensors designed to detect access violations or intrusions using sensors such as door/window

		switches, motion sensors, acoustic sensors, seismic sensors, and thermal sensors. May also include temperature sensors for critical areas.
14SW-01- ASTN	Network, Acoustic Sensor Triangulation	Network of deployed acoustic sensors and one or more processing nodes for data integration and analysis. Such networks can be set to one or more ranges of frequencies to detect sounds such as gunshots, heavy weapons discharge, explosions, man-portable air defense system launches, vehicle noises, etc., and utilize acoustic triangulation to provide accurate location data. Such networks can be wired, wireless, or hybrid, and are capable of operation near critical infrastructure assets or in wide areas.
14SW-01- DOOR	Doors and Gates, Impact Resistant	Reinforced doors and gates with increased resistance to external impact for increased physical security.
14SW- 01- LITE	Lighting, Area, Fixed	Fixed high-intensity lighting systems for improved visibility in areas such as building perimeters, parking lots, and other critical zones to increase physical security.
14SW-01- PACS	System, Physical Access Control	Locking devices and entry systems for control of physical access to facilities.
14SW-01- SIDP	Systems, Personnel Identification	Systems for positive identification of personnel as a prerequisite for entering restricted areas or accessing information systems.
14SW-01- SIDV	Systems, Vehicle Identification	Systems for identification of vehicles, ranging from decals to radio frequency identification or other transponder devices. (License plate reader and facial recognition software are NOT allowed.)
14SW-01- SNSR	Sensors/Alarms, System and Infrastructure Monitoring, Standalone	Standalone sensors/alarms for use on critical systems or infrastructure items (e.g., security systems, power supplies, etc.) to provide warning when these systems fail or are near failure.
14SW-01- VIDA	Systems, Video Assessment, Security	Camera-based security systems utilizing standard, low light, or infrared technology. (License plate reader and facial recognition software are NOT allowed.)
14SW-01- WALL	Barriers: Fences; Jersey Walls	Obstacles designed to channel or halt pedestrian or vehicle-borne traffic to protect a physical asset or facility such as barriers, bollards, planters, benches etc. (Earthen barriers, berms, trees, or other botanical obstacles are NOT allowed.)
15SC-00- PPSS	Systems, Personnel/Package Screening	Hand-held or fixed systems such as walk-through magnetometers used to screen personnel and packages for hazardous materials/devices.
21GN-00- INST	Installation	Installation costs for authorized equipment purchased through FEMA grants.
21GN-00- TRNG	Training and Awareness	See Section "Training and Exercises"

Other dropdowns in the Section IV-B of IJ, while not part of the AEL, include the following:

Code	Title
Contract Security	Private Contact Security Personnel/Guards
M&A	Management and Administration (M&A)
Planning	Planning
Exercise	Exercise
Contract Security	Private Contact Security Personnel/Guards

Unless otherwise stated, equipment must meet all mandatory statutory, regulatory, and FEMA-adopted standards to be eligible for purchase using these funds, including the Americans with Disabilities Act. In addition, recipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment, whether with NSGP funding or other sources of funds.

Recipients and subrecipients may purchase equipment not listed on the AEL, but only if they first seek and obtain prior approval from FEMA. **Note:** Nonprofits should indicate in their budget narratives if a cost includes shipping and/or tax. It is not required to break the costs out as separate from the relevant purchase(s).

Subapplicants should analyze the cost benefits of purchasing versus leasing equipment, especially high-cost items, and those subject to rapid technical advances. Large equipment purchases must be identified and explained. For more information regarding property management standards for equipment, please reference 2 C.F.R. Part 200, including but not limited to 2 C.F.R. §§ 200.310, 200.313, and 200.316. Also see 2 C.F.R. §§ 200.216, 200.471, and FEMA Policy #405-143-1 – Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services.

FEMA Policy #405-143-1, Prohibitions on Expending FEMA Award Funds for Covered Telecommunications Equipment or Services, regarding prohibitions on covered telecommunications equipment or services. Additionally, recipients that are using NSGP funds to support emergency communications equipment activities must comply with the SAFECOM Guidance on Emergency Communications Grants, including provisions on technical standards that ensure and enhance interoperable communications. This SAFECOM Guidance can be found at the Funding and Sustainment page on CISA.gov Funding Resources | CISA.

The Installation of certain equipment may trigger Environmental Planning and Historic Preservation (EHP) requirements. Please reference the EHP sections in this NOFO and the FEMA Preparedness Grant Manual - 2024 for more information. Additionally, some equipment installation may constitute construction or renovation. Please see the Construction and Renovation subsection for additional information.

TRAINING AND EXERCISES

Training and exercise costs are allowed under this program only as described in this funding notice and the FEMA Preparedness Grant Manual - 2024.

Nonprofit organizations may use NSGP funds for the following training-related costs:

a) Employed or volunteer security staff to attend security-related training within the United States;
b) Employed or volunteer staff to attend security-related training within the United States with the intent of training other employees or members/congregants upon completing the training (i.e., “train-the-trainer” type courses); and
c) Nonprofit organization’s employees, or members/congregants to receive on- site security training.

Allowable training-related costs under the NSGP are limited to attendance fees for training and related expenses, such as materials, supplies, and/or equipment. Overtime, backfill, and travel expenses are **not** allowable costs.

Allowable training topics are limited to the protection of critical infrastructure key resources, including physical and cybersecurity, facility hardening, and terrorism/other extremism awareness/employee preparedness such as Community Emergency Response Team (CERT) training, indicators and behaviors indicative of terrorist/other extremist threats, Active Shooter training, and emergency first aid training. Additional examples of allowable training courses include: “Stop the Bleed” training, kits/equipment, and training aids; First Aid and other novice

level "you are the help until help arrives" training, kits/equipment, and training aids; and Automatic External Defibrillator (AED) and AED/Basic Life Support training, kits/equipment, and training aids.

Training conducted using NSGP funds must address a specific threat and/or vulnerability, as identified in the nonprofit organization's Investment Justification (IJ). Training should provide the opportunity to demonstrate and validate skills learned as well as to identify any gaps in these skills. Proposed attendance at training courses and all associated costs using the NSGP must be included in the nonprofit organization's IJ.

Funding may be used to conduct security-related exercises. This includes costs related to planning, meeting space and other meeting costs, facilitation costs, materials and supplies, and documentation. Exercises afford organizations the opportunity to validate plans and procedures, evaluate capabilities, and assess progress toward meeting capability targets in a controlled, low risk setting. All shortcomings or gaps—including those identified for children and individuals with access and functional needs—should be identified in an improvement plan. Improvement plans should be dynamic documents with corrective actions continually monitored and implemented as part of improving preparedness through the exercise cycle.

The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. For additional information on HSEEP, refer to Homeland Security Exercise and Evaluation Program | FEMA.gov. In accordance with HSEEP guidance, subrecipients are reminded of the importance of implementing corrective actions iteratively throughout the progressive exercise cycle. This link provides access to a sample After Action Report (AAR)/Improvement Plan (IP) template: Improvement Planning – HSEEP Resources – Preparedness Toolkit (fema.gov). Recipients are encouraged to enter their exercise data and AAR/IP in the Preparedness Toolkit.

MAINTENANCE AND SUSTAINMENT

Maintenance and sustainment costs, such as maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable. For additional information, see FEMA Preparedness Grant Manual - 2024.

CONSTRUCTION AND RENOVATION

NSGP funding may not be used for construction and renovation projects without prior written approval from FEMA. In some cases, the installation of equipment may constitute construction and/or renovation. If you have any questions regarding whether an equipment installation project could be considered construction or renovation, please contact the DHSEM Grants Manager. All recipients of NSGP funds must request and receive prior approval from FEMA before any NSGP funds are used for any construction or renovation. Additionally, sub recipients are required to submit a budget and budget detail citing the project costs and an SF-424D Form for standard assurances for the construction project. The total cost of any construction or renovation paid for using NSGP funds may not exceed 15% of the NSGP award.

CONTRACTED SECURITY PERSONNEL

Contracted security personnel are allowed under this program only as described in this NOFO and must comply with guidance set forth in IB 421b and IB 441IB, 421b, IB 441. NSGP funds may not be used to purchase equipment for contracted security.

REVIEW AND RECOMMENDATION TO DHS/FEMA

a) The NMDHSEM's Grants Management Bureau uses the attached Nonprofit Security Grant Program Scoring

Matrix – Fiscal Year 2024 to review and score all investment justifications for eligibility, completeness and to validate compliance with both the Federal NOFO and State Funding Announcement.

b) The NMDHSEM Grants Support Unit will contact each applicant that needs to submit additional 'proof' or 'back-up.' To meet the requirement for a grant award, there is a 72-hour turn-around required for the submittal of these materials.
c) Investment Justifications that meet the criteria established in the attached Nonprofit Security Grant Program Scoring Matrix – Fiscal Year 2024, Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2024 Nonprofit Security Grant Program and the FEMA Preparedness Grant Manual - 2024 will be submitted by NMDHSEM to DHS/FEMA for final approval and allocation of funds.
d) Award letters are sent to applicants that are allocated funding. Letters will also be sent to applicants that do not receive funding and will include a description of why activities were not selected for funding. It is anticipated that these letters will be sent within 45 – 60 days of NMDHSEM's receipt of the NSGP award.
e) For those communities that are allocated funding, a Sub-grant Agreement will be sent. As the Sub-grant Agreement can be sent only after FEMA awards funding to the State, the distribution date will be within 45 – 60 days of NMDHSEM's receipt of the NSGP award.

N. Submitting the Application

a) Read this Funding and Allocation Methodology.
b) Review the FY 2024 NSGP Subapplicant Quick Start Guide and The U. S. Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2024 Nonprofit Security Grant Program
c) Read the FEMA Preparedness Grant Manual - 2024.
d) If beneficial for your organization, request technical assistance from the NMDHSEM Grants Management dhsem-grantsmanagement@state.nm.us. Be sure to include **NSGP 2024 Grant Program** in the subject line of your email.
e) Prepare and submit and email the attached Nonprofit Security Grant Program Investment Justification *(FEMA Form FF-207-FY-21-115 [formerly 089-25] OMB No. 1660-0163 Expiration: 09/30/2024)*, NM DHSEM Supplemental Application, Budget Worksheet and all supporting documentation to NM DHSEM Grants Management Bureau, dhsem-grantsmanagement@state.nm.us **no later than close of business at 5:00 p.m. on June 3, 2024**. Be sure to include **NSGP 2024 Grant Program Application – Applicant Name** in the subject line. **Applications submitted after 5:00 p.m. on June 3, 2024, will not be accepted.**
a) For the investment justification and supplemental NM DHSEM application, an electronic certified signature is acceptable. Scan of hard copy wet ink signatures is also acceptable.
b) If there are extenuating circumstances that do not allow for the submittal deadline to be met, applicants may request a written extension with justification for the delay. The request should be addressed to the NM DHSEM Grants Management dhsem-grantsmanagement@state.nm.us. Be sure to include **NSGP 2024 Grant Program Extension Request**, in the subject line. The extension must be submitted no later than close of business, 5:00 p.m. on May 24, 2024. The maximum extension will be one week and if approved, the extension deadline would then be June 7, 2023. Extension requests will be granted only due to compelling operational challenges.

O. Important Dates

Deadline	Description
April 23, 2024	Release of NSGP 2024 State Funding Announcement and Allocation Methodology, and Application
May 6, 2024	FY 2024 NSGP Webinar

June 3, 2024	FY 2024 NSGP Application due to NM DHSEM by Close of Business 5:00 p.m.
June 4-7, 2024	NM DHSEM Review of Investment Justifications and Request for Information (RFI) process
June 10 – 14, 2024	NSGP Investment Justifications Review Process
June 24, 20024	NMDHSEM State FY 2024 NSGP application due to FEMA
45 – 60 days following FEMA's award of funds to State; award and denial letters sent to applicants	
45 – 60 days following FEMA's award of funds to State; Sub-grants awarded to applicants (Sub-grants will be sent only after FEMA awards the grant to State)	

P. Resources:

The following are links to websites that can provide you helpful information on the 2024 Nonprofit Security Grant Program:

- FY 2024 NSGP Subapplicant Quick Start Guide
- The U. S. Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2024 Nonprofit Security Grant Program
- FY 2024 NSGP Frequently Asked Questions
- FY 2024 NSGP Fact Sheet
- FY 2024 NSGP Key Changes
- CISA Website
- How to apply

Q. NSGP Contact Information:

Marcella Benton, DHSEM Grants Manager, marcella.benton@dhsem.nm.us.
General Questions: Grants Management Bureau, dhsem-grantsmanagement@state.nm.us.

###